

1  
2  
3 UNITED STATES DISTRICT COURT  
4 WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

5 UNITED STATES OF AMERICA,

6 Plaintiff,

7 v.

8 DOUGLAS BLOUIN,

9 Defendant.

CR16-307 TSZ

ORDER

10 THIS MATTER came before the Court on four motions brought by defendant  
11 Douglas Blouin: (i) a motion to suppress, docket no. 61; (ii) a motion for a Franks  
12 hearing, docket no. 63; (iii) a motion to dismiss, suppress, or for a jury instruction  
13 regarding spoliation, docket no. 59; and (iv) a motion to exclude pursuant to Daubert,  
14 docket no. 62. By Minute Order entered July 25, 2017, docket no. 90, and by oral ruling  
15 issued on July 27, 2017, see Minutes (docket no. 91); Tr. at 96:10-99:24 (docket no. 99),  
16 the Court denied all of these motions, with the exception of the alternative request for a  
17 jury instruction regarding spoliation, which was deferred to trial. This Order incorporates  
18 by reference the Court's oral ruling and further explains the Court's reasoning.

19 **Background**

20 At issue in each of defendant's motions is the Government's deployment of  
21 software known as RoundUp eMule. Using RoundUp eMule, Homeland Security  
22 Investigations ("HSI") Special Agent Toby Ledgerwood allegedly downloaded twelve  
23

1 videos and two images of child pornography from a computer with an Internet Protocol  
2 (“IP”) address associated with defendant. After a search warrant was obtained, a Dell  
3 desktop computer was seized from defendant’s home. A forensic examination of the  
4 computer revealed that it had been “thoroughly scrubbed” just days before the search, and  
5 only one image of child pornography was found, which was not among the materials  
6 previously downloaded by Ledgerwood.<sup>1</sup>

7 RoundUp eMule was developed by Brian Lynn, a Senior Programmer in the  
8 College of Information and Computer Sciences at the University of Massachusetts,  
9 Amherst, with funding from the Department of Justice. See Lynn Decl. at ¶¶ 1-2 (docket  
10 no. 79). It is a modified version of the publicly-available (“open source”) peer-to-peer  
11 (“p2p”) file-sharing program known as eMule. See id. at ¶ 4. RoundUp eMule was first  
12 released in March 2011. Id. at ¶ 6. Lynn testified at the hearing on July 27, 2017, that  
13 sixteen (16) different versions of RoundUp eMule have been created, but not all of them  
14 were released. Version 1.54, which was used by Ledgerwood in this matter, was released  
15 in January 2015. Id. It was not, unlike Version 1.38, subjected to validation testing, see  
16 Pla.’s Hrg. Ex. 2 (Report by The MITRE Corporation), but Lynn believes that none of the  
17 intervening changes would have altered the functionality of RoundUp eMule, see Lynn  
18 Decl. at ¶ 12.

---

21 <sup>1</sup> According to defendant’s expert, the image was found in “pagefile.sys,” which is a file created and  
22 managed by the Microsoft Windows operating system, and which is not accessible to the user. See  
23 Lahman Decl. at 12 (docket no. 83-2); see also Gillie Decl. at ¶ 13 (docket no. 74-1) (indicating that a  
single image of child pornography was discovered on defendant’s hard drives, within a system file).

1 Like eMule and another open-source program known as Shareaza, RoundUp  
2 eMule adheres to the protocol of the eDonkey/KAD p2p file-sharing network, and  
3 enables downloading of only those files being shared by eDonkey/KAD clients. *See id.*  
4 at ¶¶ 7 & 9; *see also* Erdely Decl. at ¶¶ 4-5 (docket no. 38-1). Lynn has indicated under  
5 oath that he did not include any code in RoundUp eMule that would facilitate involuntary  
6 sharing of files. Lynn Decl. at ¶ 9; *see also* Erdely Decl. at ¶¶ 12, 17, 21, & 23. Lynn  
7 has also testified via declaration, as well as during the hearing on July 27, 2017, that,  
8 unlike eMule and Shareaza, RoundUp eMule downloads files from a single source to  
9 ensure that they come from one particular eDonkey/KAD network user. *See* Lynn Decl.  
10 at ¶ 10; *see also* Erdely Decl. at ¶¶ 6 & 16. In February 2014, Lynn released another  
11 program known as the RoundUp eMule Scheduler, which allows law enforcement to  
12 automate the process of downloading from single sources based on the geographic areas  
13 of IP addresses. Lynn Decl. at ¶ 13. In connection with his investigation in this matter,  
14 Ledgerwood also used the RoundUp eMule Scheduler.

## 15 **Discussion**

### 16 **A. Motion to Suppress**

17 Defendant essentially contends that law enforcement should have obtained a  
18 search warrant before deploying RoundUp eMule to download items from his computer  
19 and to obtain his IP address. The threshold question is whether the use of RoundUp  
20 eMule constituted a search. In support of his argument that a warrant was required,  
21 defendant cites a law review article for the proposition that *United States v. Jones*, 565  
22 U.S. 400 (2012), adopted a “mosaic theory” of the Fourth Amendment, pursuant to which  
23

1 the collective activities of law enforcement personnel could constitute a search even  
2 though no individual step viewed in isolation would support such conclusion. See Orin S.  
3 Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311 (2012). The  
4 premise of Kerr’s article, however, is faulty. Neither the majority opinion nor Justice  
5 Sotomayor’s concurrence endorse such “mosaic theory.”

6 In Jones, which concerned the installation of a global-positioning-system (“GPS”)  
7 tracking device on a vehicle registered to the defendant’s wife, the Supreme Court  
8 clarified that the “reasonable expectation of privacy” test articulated in Katz v. United  
9 States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring), merely augmented, see 565  
10 U.S. at 409, and “did not displace or diminish” the “trespassory test” that preceded it,  
11 id. at 414 (Sotomayor, J., concurring). Using the trespassory test, the Supreme Court  
12 concluded that, although the vehicle had been in a public place when the GPS device was  
13 attached to its undercarriage, the Government had encroached on a protected area (the  
14 vehicle itself) and a search warrant was therefore required. Id. at 410-11; see also id. at  
15 414 (Sotomayor, J., concurring) (“the trespassory test applied in the majority’s opinion  
16 reflects an irreducible constitutional minimum: When the Government physically  
17 invades personal property to gather information, a search occurs”). Contrary to Kerr’s  
18 view, Justice Sotomayor’s concurrence did not adopt a “mosaic” standard; at most, it  
19 acknowledged that the current Fourth Amendment standards, which “treat secrecy as a  
20 prerequisite for privacy,” are “ill suited to the digital age, in which people reveal a great  
21 deal of information about themselves to third parties in the course of carrying out  
22 mundane tasks.” Id. at 417-18 (Sotomayor, J., concurring). To the extent defendant  
23

1 contends that the operation of RoundUp eMule amounts to a search under some “mosaic  
2 theory,” his argument lacks jurisprudential support.

3 Defendant also relies on United States v. Darby, 190 F. Supp. 3d 520 (E.D. Va.  
4 2016), in which the deployment of a Network Investigative Technique (“NIT”) was  
5 found to constitute a search. The NIT used in Darby was sent by Government agents to  
6 computers that logged onto a particular website (Playpen) offering child pornography,  
7 and instructed such computers to transmit back certain information, including the IP  
8 address of the computer. Id. at 526-27. The Darby Court reasoned that the NIT, which  
9 was surreptitiously installed on the defendant’s computer, gave the Government access to  
10 all of the contents of the computer, in which the defendant had a reasonable expectation  
11 of privacy. Id. at 529-30.

12 RoundUp eMule is not analogous to the NIT at issue in Darby. It does not place  
13 any program on the target computer or give the Government access to anything other than  
14 the items in the “shared” folder, which are available to anyone using a similar peer-to-  
15 peer file-sharing program. Accessing files in a “shared” folder does not violate the  
16 Fourth Amendment because no reasonable expectation of privacy exists with regard to  
17 such files. See United States v. Borowy, 595 F.3d 1045, 1048 (9th Cir. 2010); see also  
18 United States v. Dreyer, 804 F.3d 1266, 1278 n.6 (9th Cir. 2015) (citing United States v.  
19 Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008)). In Borowy, the Ninth Circuit also  
20 concluded that, even if the download of files known to be associated with child  
21 pornography was a seizure, it was supported by probable cause. 595 F.3d at 1049.

22 Defendant’s contention that law enforcement was required to obtain a search warrant  
23

1 before deploying RoundUp eMule lacks merit, and as a result, his motion to suppress was  
2 denied.

3 **B. Motion for Franks Hearing**

4 Defendant challenges the search warrant issued for his residence, electronic  
5 devices, and person on grounds that the affidavit filed in support of the search warrant  
6 application was deficient in two respects: (i) failing to indicate that the process by which  
7 defendant's IP address was revealed was automated and that the system being used had  
8 not been validated; and (ii) failing to state that defendant's prior conviction for child  
9 molestation was almost 20 years old and did not involve a computer, the Internet, p2p or  
10 file-sharing technology, or child pornography.

11 An affidavit in support of a search warrant is presumptively valid. *Franks v.*  
12 *Delaware*, 438 U.S. 154, 171 (1978). To be entitled to an evidentiary hearing, defendant  
13 must make a "substantial preliminary showing that a false statement knowingly and  
14 intentionally, or with reckless disregard for the truth, was included by the affiant in the  
15 warrant affidavit." *Id.* at 155-56. Omissions meeting such standard can also require a  
16 hearing, *see United States v. Perkins*, 850 F.3d 1109, 1116 (9th Cir. 2017), but  
17 negligence or an innocent mistake is insufficient, *Franks*, 438 U.S. at 171. If defendant  
18 makes the requisite initial showing, but the affidavit remains sufficient when the alleged  
19 false statement is disregarded or the omitted information is included, then no evidentiary  
20 hearing is necessary. *Id.* at 171-72; *Perkins*, 850 F.3d at 1116 ("the false or misleading  
21 statement or omission" must be "material, *i.e.*, 'necessary to finding probable cause'").  
22  
23

1 In two different cases, the Eastern District of Wisconsin has rejected Franks  
2 arguments similar to those being made here. See United States v. Feldman, 2014 WL  
3 7653617 (E.D. Wis. July 7, 2014); United States v. Case, 2014 WL 1052946 (E.D. Wis.  
4 Mar. 17, 2014). In Feldman, the court was “not persuaded that the fact that the  
5 investigation may have occurred automatically rather than through the manual  
6 manipulation of an investigator is relevant in the court’s assessment of probable cause,”  
7 and it did not “find problematic the omission of the name of the software or every detail  
8 of its capabilities.” 2014 WL 7653617 at \*7. As recognized in Feldman, the dispositive  
9 question is whether the warrant was supported by probable cause to believe that  
10 contraband or evidence of a crime was likely to be found at the residence. Id. Probable  
11 cause does not require certainty and “demands even less than probability.” Id. at \*9  
12 (quoting United States v. Carmel, 548 F.3d 571, 576 (7th Cir. 2008)).

13 In Feldman, using RoundUp eMule, law enforcement personnel identified the  
14 defendant’s computer as responding to a request for 17 hash values of known child  
15 pornography; however, they were unable on 320 attempts to download any of the  
16 suspected files, which might have been the result of a firewall or router characteristics.  
17 Id. at \*4 & \*8. The defendant in Feldman did not contend that the failure to download  
18 the material meant the contraband or evidence was not likely to be found on the  
19 defendant’s computer or residence, id. at \*8, and the court concluded that “[s]uccessful  
20 single-source download of the suspect files was not necessary; hash value matches alone  
21 were sufficient to establish probable cause,” id. at \*10. The Feldman Court relied, in  
22 part, on a Federal Judicial Center publication stating that “‘less than one in one billion’  
23

1 chance” exists that “the two most commonly used hash algorithms will generate the same  
2 hash value for different files.” *Id.* at \*9 (quoting Barbara J. Rothstein, et al., *Managing*  
3 *Discovery of Electronic Information: A Pocket Guide for Judges* 24 (Fed. Judicial Ctr.  
4 2007)).

5 Case involved a different version of RoundUp, which was designed to work with  
6 the “Ares” p2p network. 2014 WL 1052946 at \*3. In applying for the search warrant at  
7 issue, the affiant attributed the work of RoundUp to an “online covert employee,” called  
8 “OCE5023.” *Id.* at \*2. The Case Court observed that the defendant’s arguments “did not  
9 really fit under the *Franks* framework,” but were instead more suitable as a *Murray* or  
10 *Markling* challenge, in which the search warrant is attacked because it is based on  
11 evidence recovered during a previous, unlawful search. *Id.* (citing *Murray v. United*  
12 *States*, 487 U.S. 533 (1988), and *United States v Markling*, 7 F.3d 1309 (7th Cir. 1993)).  
13 The Case Court rejected the argument that the affiant’s failure to disclose that RoundUp  
14 was running unattended at the time child pornography was downloaded from the  
15 defendant’s computer precluded a finding of probable cause, distinguishing the facts of  
16 Case from “a situation where a computer program downloaded material believed to be  
17 contraband . . . and no human being looked at the material before a warrant was sought.”  
18 *Id.* at \*4. Instead, in Case, after the images were downloaded, they were confirmed to be  
19 child pornography, and using the IP address from which the images were obtained, the  
20 defendant was identified as the subscriber via a subpoena issued to the Internet service  
21 provider. *Id.* The Case Court concluded that this process was “sufficiently reliable to  
22 support the issuance of the warrant.” *Id.*



1 The Court concludes as a matter of law that, if files with hash values known to be  
2 associated with child pornography are reported to be on the “shared” folder of a suspect’s  
3 computer, probable cause exists for searching such suspect’s computer. Because hash  
4 values are analogous to fingerprints and provide high confidence that the contents of files  
5 associated with such hash values are known, the images or videos need not themselves be  
6 downloaded from the suspect’s computer in advance of the issuance or execution of a  
7 search warrant. Thus, any question concerning whether, in this case, RoundUp eMule  
8 actually effected a single-source download from defendant’s computer does not affect the  
9 validity of the search warrant.

10 United States v. Perkins, 850 F.3d 1109 (9th Cir. 2017), and United States v.  
11 Needham, 718 F.3d 1190 (9th Cir. 2013), on which defendant relies in support of his  
12 argument that the search warrant affidavit did not disclose enough information about his  
13 prior child-molestation conviction, are both distinguishable. In Perkins, the defendant  
14 traveled through the Toronto International Airport on his way home from Chile to  
15 Washington. 850 F.3d at 1112. He was stopped by Canadian Border Services Agency  
16 officers because he was a registered sex offender. Id. A laptop he was carrying, which  
17 turned out to belong to his wife, was searched, and he was arrested for being in  
18 possession of child pornography. Id. at 1113. The next day, a Peel Regional Police  
19 Constable reviewed the two images on the laptop and concluded that they did not  
20 constitute child pornography under Canadian law. Id. The subsequent search warrant  
21 affidavit prepared by an agent of the United States Department of Homeland Security  
22 (i) omitted the fact that Canadian authorities dropped the possession of child pornography  
23

1 charge because the images were not pornographic, (ii) provided a misleading description  
2 of one of the two images, and (iii) did not attach a copy of either image. *Id.* at 1116. The  
3 *Perkins* Court held that the defendant's motion to suppress evidence obtained pursuant to  
4 the resulting search warrant was erroneously denied by the district court. *Id.* at 1123. It  
5 reasoned that, if corrected, the search warrant application would have included only  
6 copies of the non-pornographic images and the defendant's convictions for first-degree  
7 incest and for first-degree child molestation, both of which were over twenty years old,  
8 and this information would not have been enough to justify the issuance of a warrant to  
9 search the defendant's home and computers for child pornography. *Id.* at 1119-23.

10 *Needham* involved a search warrant issued for evidence of possession or  
11 distribution of child pornography on the basis of a report that the defendant was believed  
12 to be the individual who molested a five-year-old boy in a restroom at the local mall.  
13 718 F.3d at 1191-93. After the search warrant was executed, the Ninth Circuit decided  
14 *Dougherty v. City of Covina*, 654 F.3d 892 (9th Cir. 2011), in which officers were  
15 granted qualified immunity as to their improper reliance on a warrant predicated on the  
16 bare inference that persons who molest children are likely to possess child pornography.  
17 *See* 718 F.3d at 1194-95. Although the warrant in *Needham* was likewise the product of  
18 an alleged propensity of child molesters to collect child pornography, which is not alone  
19 sufficient to establish probable cause to search for such pornography, the Ninth Circuit  
20 concluded that, at the time the search warrant was executed, the law was not so clearly  
21 established as to render the officers' reliance on the warrant objectively unreasonable. *Id.*  
22 at 1195.

1 Unlike in *Perkins* and *Needham*, the search warrant affidavit at issue in this case  
2 includes much more than a bare inference drawn from a prior conviction of child  
3 molestation that the suspect possesses child pornography. In this matter, the affidavit  
4 indicates that Ledgerwood established a single-source connection with defendant's IP  
5 address and downloaded several files depicting child pornography, as defined by federal  
6 law, including two videos that Ledgerwood reviewed and described in detail in his  
7 affidavit. Ledgerwood Aff. at ¶¶ 13-20, Def.'s Ex. G (docket no. 64). In contrast to the  
8 defendant in *Perkins*, defendant here does not contend that Ledgerwood's summary of  
9 the videos is in any way misleading or that Ledgerwood omitted information that might  
10 cast doubt on whether the videos depicted child pornography. In sum, in this case, the  
11 search warrant is not improperly premised solely on a prior conviction for child  
12 molestation; rather, the reference to defendant's prior conviction simply provides a basis  
13 for distinguishing between defendant and any other individual who might share the IP  
14 address at issue for purposes of searching the person, as opposed to the premises,  
15 identified in the search warrant. Defendant has not made the requisite showing for a  
16 *Franks* hearing, and his motion was therefore denied.

17 **C. Motion to Dismiss**

18 Defendant previously sought to compel the Government to produce the source  
19 code for Version 1.54 of RoundUp eMule. Based on the facts represented at the time in  
20 the parties' briefing, the Court denied defendant's motion. *See* Order (docket no. 56).  
21 The facts now appear to be slightly different from what was earlier understood, and  
22 defendant has renewed his request for the source code, which is addressed in the next  
23

1 section concerning his Daubert motion. The most significant change in the parties'  
2 recitations of facts involves whether eMule and Shareaza were installed on defendant's  
3 computer. Although the Government indicated in its response to defendant's motion to  
4 compel that both programs were installed on his computer, see Pla.'s Resp. at 7:2 (docket  
5 no. 38), the parties seem to currently agree that the programs had been downloaded, but  
6 were either not configured or not installed, see Gillie Decl. at 12 (eMule and Shareaza  
7 had not been configured); see also Lahman Decl. at 19 (docket no. 83-2) (Shareaza was  
8 not installed; eMule was installed, but never executed and configured).

9       This information was evidently known as early as November 10, 2016, when  
10 HSI Computer Forensics Analyst Thomas Gillie engaged in a direct, non-write-blocked  
11 interaction with the hard drives seized from defendant's residence. See Gillie Decl. at  
12 ¶¶ 7-13. He did so to answer what he believed were time-sensitive questions from  
13 Ledgerwood, who was in the process of testifying before the grand jury from which an  
14 indictment in this case was being solicited. See id. at ¶ 7; see also Def.'s Ex. H (docket  
15 no. 83-1). In a responsive text to Ledgerwood, Gillie wrote that he found the Shareaza  
16 program on defendant's computer, but when he started the application, it began by  
17 "asking to select setup language." Def.'s Ex. L (docket no. 83-4). Gillie speculated: "I  
18 bet he deletes the program after he downloads." Id. Gillie did not himself add, alter, or  
19 delete any files or settings, but his examination of defendant's computer caused the  
20 operating system to modify over 700 files. See Gillie Decl. at ¶¶ 11-12. Although an  
21 exact copy of each hard drive had been made before Gillie's analysis on November 10,  
22  
23

2016, and were preserved, defendant has accused Gillie of spoliating evidence and seeks as a remedy dismissal, suppression, or a jury instruction regarding spoliation.

The Government's failure to preserve potentially exculpatory evidence rises to the level of a due process violation if the Government acted in bad faith. United States v. Flyer, 633 F.3d 911, 916 (9th Cir. 2011). Bad faith requires more than mere negligence or recklessness. Id. If the Government destroys evidence under circumstances that do not constitute a violation of a defendant's constitutional rights, the Court may still impose sanctions, including the suppression of secondary evidence. Id. In deciding whether to impose sanctions, the Court must balance "the quality of the Government's conduct and the degree of prejudice to the accused." Id. The Government bears the burden of justifying its conduct and the defendant bears the burden of demonstrating prejudice. Id.

Although Gillie might have used alternative means to answer the questions posed by the grand jury, no showing has been made that he, Ledgerwood, or Assistant United States Attorney Matthew Hampton affirmatively altered, or acted in bad faith to alter, the hard drive. Moreover, defendant has not explained what exculpatory evidence on the hard drive was or might have been spoliated. Any previously deleted child pornography that might have been overwritten during the course of Gillie's examination would be inculpatory, not exculpatory. Given the relative innocuousness of the Government's conduct and the lack of apparent prejudice to defendant, neither dismissal nor suppression of evidence would be an appropriate sanction. Whether to give a jury instruction regarding spoliation turns on the evidence presented at trial, and the issue was therefore deferred.

1 **D. Motion to Exclude Pursuant to *Daubert***

2 Defendant moved to exclude testimony concerning RoundUp eMule pursuant to  
3 *Daubert v. Merrell Dow Pharms., Inc.*, 509 U.S. 579 (1993), and *Kumho Tire Co. v.*  
4 *Carmichael*, 526 U.S. 137 (1999). *Daubert* and *Kumho* provide standards for expert  
5 testimony. Expert testimony is admissible pursuant to Federal Rule of Evidence 702 if it  
6 is both relevant and reliable.<sup>2</sup> E.g., *Estate of Barabin v. AstenJohnson, Inc.*, 740 F.3d  
7 457, 463 (9th Cir. 2014) (en banc). The Court has an obligation to act as “gatekeeper” to  
8 exclude “junk science” that does not meet Rule 702’s reliability standard. *Id.* The  
9 *Daubert* list of non-exhaustive factors for assessing the reliability of expert testimony  
10 includes: (i) whether a theory or technique can be (and has been) tested; (ii) whether the  
11 theory or technique has been subjected to peer review and publication; (iii) whether the  
12 theory or technique has a known or potential error rate; and (iv) whether the theory or  
13 technique is generally accepted in the relevant scientific community. *Id.*; see *Daubert*,  
14 509 U.S. at 593-94. The Court may disregard some of these factors and/or consider other  
15 factors, depending on the particular circumstances of a particular case; the Rule 702  
16 inquiry is “flexible” and *Daubert* does not set forth a “definitive checklist or test.” See  
17 *Kumho*, 526 U.S. at 141-42 & 149-52.

---

18 <sup>2</sup> Rule 702 was amended in 2000 and restyled in 2011, and now reads as follows:

19 A witness who is qualified as an expert by knowledge, skill, experience, training, or  
20 education may testify in the form of an opinion or otherwise if:

- 21 (a) the expert’s scientific, technical, or other specialized knowledge will help the trier  
22 of fact to understand the evidence or to determine a fact in issue;
- 23 (b) the testimony is based on sufficient facts or data;
- (c) the testimony is the product of reliable principles and methods; and
- (d) the expert has reliably applied the principles and methods to the facts of the case.

1 With regard to Ledgerwood, who would be a fact or lay witness with respect to his  
2 use of RoundUp eMule, neither Daubert nor Kumho apply. Ledgerwood will be  
3 permitted to testify about how he interfaced with the RoundUp eMule program and what  
4 resulted from his efforts. Ledgerwood does not have to know about or explain how the  
5 program executes its source code; he just has to describe the manner in which he used it.  
6 To the extent defendant argues otherwise, the natural extension of his reasoning would be  
7 to require that a state trooper or highway patrol officer know about and be able to explain  
8 the science underlying a radar gun and how one is constructed before being allowed to  
9 testify about the vehicle speed that was measured using such device. The law does not  
10 require law enforcement personnel using technology to perform their work (for example,  
11 field tests for controlled substances, blood-alcohol content measurement devices) to be  
12 qualified as experts before they can testify about their observations. To the extent the  
13 reliability (and perhaps relevance) of a particular technology is in doubt, the method for  
14 raising such challenge is not through the exclusion of the lay witnesses who used the  
15 technology.

16 As to Lynn, defendant cannot seriously challenge his expertise or his ability to  
17 testify about how he created the program, what the program is designed to do, and  
18 whether, in his opinion, the program does what was intended. Computer programming is  
19 not a scientific theory or technique, it is not new or novel, and it does not implicate the  
20 Court's responsibility to keep "junk science" out of the courtroom. Any doubts about  
21 whether RoundUp eMule operates in the manner that Lynn represents go to the weight,  
22 and not the admissibility, of his testimony.

1 With respect to Detective Robert Erdely, who seems to be a fact witness, rather  
2 than an expert witness, defendant's motion to exclude also lacks merit. Erdely is  
3 proffered by the Government to describe the process for training law enforcement  
4 personnel to use RoundUp eMule and to discuss the tests he has performed both as part of  
5 the training curriculum and during the course of this case. Erdely need not be a software  
6 engineer or have training in computer programming to testify about how a user interfaces  
7 with RoundUp eMule and the types of results that can be obtained. Neither Daubert nor  
8 Kumho preclude Erdely's testimony.

9 The real issue in this case does not involve Daubert and Kumho, but rather is best  
10 summed up in Feldman. In Feldman, the court observed that the defendant was "not  
11 charged for conduct the investigator observed over the peer-to-peer network but rather  
12 [for] what the investigators found in his home." 2014 WL 7653617 at \*6. In other  
13 words, in Feldman, neither RoundUp eMule nor the investigator were "transactional  
14 witnesses" to the charged offense. Id.; see also id. at \*5 ("the defendant, unlike the  
15 defendant in Budziak,<sup>3</sup> is not charged with any conduct that law enforcement observed  
16 via RoundUp"). In contrast, in this case, the evidence against defendant consists  
17 primarily of the files Ledgerwood allegedly pulled, via RoundUp eMule, from  
18 defendant's IP address. Thus, the dispositive question in this matter is whether RoundUp  
19 eMule operates in the manner asserted by the Government and engages in single-source  
20 downloading. RoundUp eMule and its operator (Ledgerwood) are, in essence, the  
21 witnesses against defendant, and the question before the Court is what discovery must

---

22 <sup>3</sup> United States v. Budziak, 697 F.3d 1105 (9th Cir. 2012).



1 defendant be provided concerning RoundUp eMule for defendant to be able to confront  
2 his accusers and adequately prepare for cross-examination.

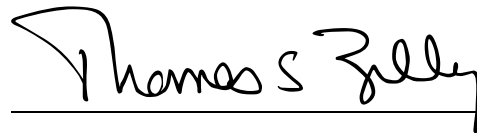
3       The Court remains persuaded that defendant does not need the source code to  
4 mount his defense. As indicated in the Order denying defendant's motion to compel,  
5 unlike the defendant in Budziak, defendant here does not contend that the program at  
6 issue allows law enforcement to modify the sharing settings on target computers.  
7 Instead, he challenges the reliability of the single-source downloading feature of  
8 RoundUp eMule. Defendant's expert suggests that, in April 2016, Ledgerwood might  
9 have downloaded the child pornography at issue from a computer that was no longer at  
10 the IP address in October 2016, when the search warrant was executed, or from one or  
11 more IP addresses other than the one associated with defendant. See Lahman Decl. at 14  
12 (docket no. 83-2). Defendant's expert has also acknowledged the possibility that  
13 Ledgerwood obtained the child pornography at issue from defendant's computer before it  
14 was deleted by defendant. See id. at 13-14. This latter explanation does not support an  
15 assertion of innocence. All of these scenarios, however, are premised not on the  
16 functionality of RoundUp eMule, but on the fact that none of the images or videos  
17 Ledgerwood captured in April 2016 were found on defendant's seized hard drives.  
18 Defendant can present these theories, the first of which is potentially exculpatory and the  
19 second of which might raise a reasonable doubt, without access to the source code, and  
20 he has not shown how having the source code would aid in his defense. Thus, to the  
21 extent defendant seeks reconsideration of the Order entered June 14, 2017, docket no. 56,  
22 such request is denied.

1 **Conclusion**

2 For the foregoing reasons, defendant's motions to suppress, docket no. 61, for a  
3 Franks hearing, docket no. 63, and to exclude pursuant to Daubert, docket no. 62, were  
4 DENIED, and defendant's motion to dismiss, suppress, or for a jury instruction regarding  
5 spoliation, docket no. 59, was DENIED in part and DEFERRED in part.

6 IT IS SO ORDERED.

7 Dated this 14th day of August, 2017.

8  
9 

10 Thomas S. Zilly  
11 United States District Judge  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23